SCALLEX

WATERLOO REGION MANUFACTURING

# Manufacturer Backup Recoverability Checklist

A practical worksheet for Waterloo Region manufacturers to distinguish backup existence from documented, tested recovery evidence.

- Inventory business-critical systems and the business functions that depend on them.
- Review backup coverage, restore-test evidence, dependencies, recovery ownership and ransomware-recovery questions.
- Turn unknowns into a prioritized recovery-readiness action list.

This resource is not a guarantee of recoverability, uptime, RPO/RTO performance or ransomware protection. It does not assess OT/ICS engineering. Do not record passwords, encryption keys, privileged credentials or sensitive network/security secrets in this worksheet.

# How to use this checklist

A backup job can exist without proving that the business can restore the right system, data and dependencies when an outage or cyber incident occurs. This worksheet focuses on evidence: what has been tested, what is only documented, and what is still unknown.

| Tested | Documented | Unknown | N/A |
|---|---|---|---|
| There is recent evidence from a restore or recovery exercise that the item worked as expected for the tested scope. | The method or coverage is documented, but the current recovery result has not been demonstrated. | The organization cannot currently confirm coverage, ownership, dependency or test evidence. | The question genuinely does not apply to the system or business function. |

**Recoverability, in this checklist: the ability to restore the data, system and supporting dependencies needed to resume a defined business function. The evidence required depends on the actual environment and recovery objectives.**

## Checklist boundary

This worksheet covers business IT recovery questions. It does not claim specialized OT/ICS security engineering and does not set universal recovery-time or recovery-point targets for manufacturers.

# 1. Critical-system recovery inventory

List the systems or services whose loss would materially interrupt office, warehouse, plant-support or customer-facing work. Use business names first; technical details can be added separately by the responsible IT team.

| System / service | Business function | Owner | Priority | Backup coverage known? |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Dependency prompts

For each critical system, identify dependencies that could prevent recovery even if data is available: identity/authentication, server or storage, network, internet/WAN, DNS, licensing, vendor access, application services, and required endpoints. Only include dependencies that actually exist in your environment.

# 2. Backup coverage and ownership

Mark the evidence state that best reflects what can be demonstrated today. “Documented” is useful, but it is intentionally different from “Tested.”

| Review question / evidence prompt | Tested | Documented | Unknown | N/A |
|---|---|---|---|---|
| 01 Can the organization identify which critical systems and data are included in backup coverage? | ☐ | ☐ | ☐ | ☐ |
| 02 Can the organization identify important systems, databases, files or SaaS data that are outside the current backup scope? | ☐ | ☐ | ☐ | ☐ |
| 03 Is there a named owner responsible for monitoring backup success/failure and unresolved exceptions? | ☐ | ☐ | ☐ | ☐ |
| 04 Are retention and recovery-copy decisions documented for critical systems rather than assumed? | ☐ | ☐ | ☐ | ☐ |
| 05 Is at least one recovery copy protected so the same incident affecting production is less likely to affect every recovery copy? | ☐ | ☐ | ☐ | ☐ |
| 06 Can the organization identify who can access or alter backup configuration and recovery data? | ☐ | ☐ | ☐ | ☐ |

# 3. Restore-test evidence

Mark the evidence state that best reflects what can be demonstrated today. “Documented” is useful, but it is intentionally different from “Tested.”

| Review question / evidence prompt | Tested | Documented | Unknown | N/A |
|---|---|---|---|---|
| 01 Has the organization performed a recent restore test for at least one representative critical workload? | ☐ | ☐ | ☐ | ☐ |
| 02 Did the test verify that restored data was usable, not only that a backup job completed? | ☐ | ☐ | ☐ | ☐ |
| 03 Were application, database or system dependencies included when they were necessary for the tested business function? | ☐ | ☐ | ☐ | ☐ |
| 04 Were test results, exceptions and follow-up actions documented? | ☐ | ☐ | ☐ | ☐ |
| 05 Can the organization identify the last successful test date and the scope that was actually tested? | ☐ | ☐ | ☐ | ☐ |
| 06 Is there a repeatable process for scheduling or triggering future recovery tests based on business need and risk? | ☐ | ☐ | ☐ | ☐ |

# 4. Recovery priorities and dependencies

Mark the evidence state that best reflects what can be demonstrated today. “Documented” is useful, but it is intentionally different from “Tested.”

| Review question / evidence prompt | Tested | Documented | Unknown | N/A |
|---|---|---|---|---|
| 01 Has leadership identified which business functions should be restored before lower-priority systems? | ☐ | ☐ | ☐ | ☐ |
| 02 Can the IT team map each priority business function to the systems and data it depends on? | ☐ | ☐ | ☐ | ☐ |
| 03 Are identity and administrator-access dependencies included in the recovery plan where required? | ☐ | ☐ | ☐ | ☐ |
| 04 Are network, firewall, internet/WAN or name-resolution dependencies included where required? | ☐ | ☐ | ☐ | ☐ |
| 05 Are vendor, licensing or application-support dependencies documented for systems that require them? | ☐ | ☐ | ☐ | ☐ |
| 06 Can the business distinguish a desired recovery target from a recovery capability that has actually been tested? | ☐ | ☐ | ☐ | ☐ |

# 5. Ransomware-recovery questions

Mark the evidence state that best reflects what can be demonstrated today. “Documented” is useful, but it is intentionally different from “Tested.”

| Review question / evidence prompt | Tested | Documented | Unknown | N/A |
|---|---|---|---|---|
| 01 Could a compromised administrator account reach or alter every backup/recovery copy? | ☐ | ☐ | ☐ | ☐ |
| 02 Is there a documented path to restore critical data or systems from recovery copies that are protected from routine production access? | ☐ | ☐ | ☐ | ☐ |
| 03 Can the organization identify how clean systems, credentials and access would be established before restoring data after a cyber incident? | ☐ | ☐ | ☐ | ☐ |
| 04 Are recovery procedures separated from ordinary production administration where the environment requires it? | ☐ | ☐ | ☐ | ☐ |
| 05 Has the organization considered how ransomware or destructive activity could affect shared storage, virtualization, identity and backup systems together? | ☐ | ☐ | ☐ | ☐ |
| 06 Are incident-response and recovery ownership roles clear enough to avoid conflicting actions during an outage? | ☐ | ☐ | ☐ | ☐ |

# 6. Vendor, documentation and escalation ownership

Mark the evidence state that best reflects what can be demonstrated today. “Documented” is useful, but it is intentionally different from “Tested.”

| Review question / evidence prompt | Tested | Documented | Unknown | N/A |
|---|---|---|---|---|
| 01 Is there a current list of vendors or support providers required to recover critical business systems? | ☐ | ☐ | ☐ | ☐ |
| 02 Can authorized staff access recovery documentation if the usual IT contact is unavailable? | ☐ | ☐ | ☐ | ☐ |
| 03 Are support contracts, license information and escalation contacts documented where recovery depends on them? | ☐ | ☐ | ☐ | ☐ |
| 04 Is vendor remote access reviewed and controlled rather than left permanently open without clear ownership? | ☐ | ☐ | ☐ | ☐ |
| 05 Can leadership identify who is authorized to declare a recovery event and prioritize restoration work? | ☐ | ☐ | ☐ | ☐ |
| 06 Are unresolved recovery gaps assigned to a named owner and next action? | ☐ | ☐ | ☐ | ☐ |

# Restore-test evidence worksheet

Use one row per recovery test. Record the real scope and result; do not mark an entire environment “tested” because one file or one system was restored successfully.

| System / workload | Test date | What was restored? | Result / exception | Next action / owner |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Questions to ask your current IT provider

| Question | Evidence / follow-up |
|---|---|
| Which critical systems are protected today, and which are not? | |
| What was the most recent restore test, and what exactly was restored? | |
| Which dependencies could prevent a recovery even if the backup data is intact? | |
| How are recovery copies protected from the same event that affects production? | |
| Who owns the recovery plan, vendor escalation and post-test remediation? | |

# Priority action worksheet

Use this page to convert unknowns into a small number of concrete recovery-readiness actions.

| Priority | Gap / unknown | Business impact | Owner | Next evidence / action |
|---|---|---|---|---|
| Now | | | | |
| Now | | | | |
| Next | | | | |
| Next | | | | |
| Later | | | | |
| Later | | | | |

## What this checklist does - and does not - tell you

It helps you: inventory critical systems, distinguish documented coverage from tested recovery, identify dependencies, clarify ownership and prepare for a deeper business IT continuity review.

It does not: guarantee recovery, set universal RPO/RTO targets, certify ransomware resilience, validate a specific backup product, or assess OT/ICS engineering.

# Reference notes reviewed August 17, 2026

CISA recommends maintaining protected backups and regularly testing backup availability/integrity for ransomware recovery. NIST contingency-planning guidance also covers backup, recovery, testing and maintenance. These are general technical references; the right recovery design and test scope still depend on the actual business environment.

CISA - #StopRansomware Guide
NIST SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

## Turn recovery unknowns into a practical IT review

If this checklist reveals unclear coverage, restore evidence or dependencies, the canonical next step is the Scallex Free IT Assessment. The assessment is separate from this worksheet and is intended to review the broader business IT context behind the unknowns you identified.

Start the Free IT Assessment at scallex.ca